

What is claimed is:

1. A network comprising:

IPsec processing apparatuses, which use an IPsec (Internet
Protocol security protocol) for securing security on the Internet
5 path in the case where different two centers communicate via
the Internet; and

an IPsec setting server apparatus, which manages IPsec
settings of said IPsec processing apparatuses,

wherein said IPsec setting server apparatus includes means
10 for collectively managing policies of said IPsec to be applied
between first and second IPsec processing apparatuses.

2. The network according to claim 1,

wherein said IPsec setting server apparatus includes means
for specifying policies of said IPsec to be applied between said
15 first and second IPsec processing apparatuses based upon contents
of a request message for communication between said first and
second IPsec processing apparatuses received from said first
IPsec processing apparatus.

3. The network according to claim 2,

20 wherein said IPsec setting server apparatus includes means
for, upon receiving the request message, transmitting a request
startup message to said second IPsec processing apparatus, which
is an opposite party of communication of said first IPsec
processing apparatus which has transmitted the request message,

in order to cause said second IPsec processing apparatus to transmit a request message for the communication.

4. The network according to claim 3,

wherein said IPsec setting server apparatus includes means
5 for, when there is no response to the request startup message,
notifying said first IPsec processing apparatus that there is
no response from said second IPsec processing apparatus.

5. The network according to claim 2,

wherein said IPsec setting server apparatus includes means
10 for generating SA (Security Association) parameters to be
required in the IPsec communication from contents of the request
message and contents of the policies of said IPsec to be applied
to the communication.

6. The network according to claim 2,

15 wherein said IPsec setting server apparatus includes means
for sending a distribution message including at least the policies
of said IPsec and the SA parameters in response to the request
message.

7. The network according to claim 1,

20 wherein said IPsec setting server apparatus includes means
for generating a common secret key to be used in encryption and
authentication of said IPsec and means for distributing the
generated common secret key to said IPsec processing apparatus.

8. An IPsec setting server apparatus managing IPsec setting of IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Internet path in the case where different two centers communicate via the Internet,

wherein said IPsec setting server apparatus includes means for collectively managing policies of said IPsec to be applied among said IPsec processing apparatuses.

9. The IPsec setting server apparatus according to claim 8, wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between an IPsec processing apparatus and another IPsec processing apparatus based upon contents of a request message for communication between said IPsec processing apparatus and another IPsec processing apparatus received from said IPsec processing apparatus.

10. The IPsec setting server apparatus according to claim 9, wherein said IPsec setting server apparatus includes means for, upon receiving the request message, transmitting a request startup message to an IPsec processing apparatus, which is an opposite party of communication of an IPsec processing apparatus which has transmitted the request message, in order to cause said IPsec processing apparatus of the opposite party of communication to transmit a request message for the communication.

11. The IPsec setting server apparatus according to claim 10,
wherein said IPsec setting server apparatus includes means
for, when there is no response to the request startup message,
notifying said IPsec processing apparatus which has transmitted
5 the request message that there is no response from said IPsec
processing apparatus of the opposite party of communication.

12. The IPsec setting server apparatus according to claim 9,
wherein said IPsec setting server apparatus includes means
for generating SA (Security Association) parameters to be
10 required in the IPsec communication from contents of the request
message and contents of the policies of said IPsec to be applied
to the communication.

13. The IPsec setting server apparatus according to claim 9,
wherein said IPsec setting server apparatus includes means
15 for transmitting a distribution message including at least the
policies of said IPsec and the SA parameters in response to the
request message.

14. The IPsec setting server apparatus according to claim 8,
wherein said IPsec setting server apparatus includes means
20 for generating a common secret key to be used in encryption and
authentication of said IPsec and a function for distributing
the generated common secret key to said IPsec processing
apparatus.

15. An IPsec processing apparatus using an IPsec (Internet Protocol security protocol) on the Internet,

wherein said IPsec processing apparatus includes means for, upon receiving a packet to which said IPsec should be applied, 5 judging whether or not to inquire a setting for said IPsec to be collectively managed in an IPsec setting server apparatus from said IPsec setting server apparatus.

16. The IPsec processing apparatus according to claim 15,

wherein said IPsec processing apparatus includes means for 10 transmitting a request message for communication with another IPsec processing apparatus to said IPsec setting server apparatus in order to acquire a setting for said IPsec.

17. The IPsec processing apparatus according to claim 16,

wherein, upon receiving a request startup message for 15 causing said IPsec processing apparatus to transmit the request message from said IPsec setting server apparatus, said IPsec processing apparatus transmits the request message.

18. The IPsec processing apparatus according to claim 15,

wherein said IPsec processing apparatus includes means for 20 setting an SPD, in which policies for applying said IPsec is recorded, and an SAD, in which an SA (security Association) necessary for subjecting an individual kind of communication to processing of said IPsec, based upon a distribution message received from said IPsec setting server apparatus.

19. The IPsec processing apparatus according to claim 15,
wherein said IPsec processing apparatus includes means for
acquiring a common secret key to be used in encryption and
authentication of said IPsec from said IPsec setting server
5 apparatus.

20. The IPsec processing apparatus according to claim 15,
wherein said IPsec processing apparatus includes means for
retransmitting the request message to said IPsec setting server
apparatus and acquiring new setting information before a term
10 of validity of the SA expires.

21. An IPsec setting method for a network which comprises: IPsec
processing apparatuses, which use an IPsec (Internet Protocol
security protocol) for securing security on the Internet path
in the case where different two centers communicate via the
15 Internet; and an IPsec setting server apparatus, which manages
IPsec settings of said IPsec processing apparatuses,
wherein said IPsec setting server apparatus includes a step
of collectively managing policies of said IPsec to be applied
among said IPsec processing apparatuses.

20 22. The IPsec setting method according to claim 21,
wherein said IPsec setting server apparatus includes a step
of specifying policies of said IPsec to be applied between an
IPsec processing apparatus and another IPsec processing
apparatus based upon contents of a request message for
25 communication between said IPsec processing apparatus and

another IPsec processing apparatus received from said IPsec processing apparatus.

23. The IPsec setting method according to claim 22,
wherein said IPsec setting server apparatus includes a step
5 of, upon receiving the request message, sending a request startup
message to an IPsec processing apparatus, which is an opposite
party of communication of an IPsec processing apparatus which
has transmitted the request message, in order to cause said IPsec
processing apparatus of the opposite party of communication to
10 transmit a request message for the communication.

24. The IPsec setting method according to claim 23,
wherein said IPsec setting server apparatus includes a step
of, when there is no response to the request startup message,
notifying said IPsec processing apparatus which has transmitted
15 the request message that there is no response from said IPsec
processing apparatus of the opposite party of communication.

25. The IPsec setting method according to claim 22,
wherein said IPsec setting server apparatus includes a step
of generating SA (Security Association) parameters to be required
20 in the IPsec communication from contents of the request message
and contents of the policies of said IPsec to be applied to the
communication.

26. The IPsec setting method according to claim 22,

wherein said IPsec setting server apparatus includes a step of transmitting a distribution message including at least the policies of said IPsec and the SA parameters in response to the request message.

5 27. The IPsec setting method according to claim 21,

 wherein said IPsec setting server apparatus includes a step of generating a common secret key to be used in encryption and authentication of said IPsec and a step of distributing the generated common secret key to said IPsec processing apparatus.

10 28. The IPsec setting method according to claim 21,

 wherein, upon receiving a packet to which said IPsec should be applied, said IPsec processing apparatus judges whether or not to inquire a setting for said IPsec to be collectively managed in an IPsec setting server apparatus from said IPsec setting
15 server apparatus.

29. The IPsec setting method according to claim 21,

 wherein said IPsec processing apparatus transmits a request message for communication with another IPsec processing apparatus to said IPsec setting server apparatus in order to
20 acquire a setting for said IPsec.

30. The IPsec setting method according to claim 21,

 wherein said IPsec processing apparatus sets an SPD, in which policies for applying said IPsec is recorded, and an SAD, in which an SA (Security Association) necessary for subjecting

an individual kind of communication to processing of said IPsec,
based upon a distribution message received from said IPsec setting
server apparatus.

31. The IPsec setting method according to claim 21,
5 wherein said IPsec processing apparatus acquires a common
secret key to be used in encryption and authentication of said
IPsec from said IPsec setting server apparatus.

32. The IPsec setting method according to claim 21,
wherein said IPsec processing apparatus resends the request
10 message to said IPsec setting server apparatus and acquires new
setting information before a term of validity of the SA expires.